UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/830,530	09/19/2001	Anthony Tung Shuen Ho	A34178PCTUSA	9690

21003 7590 06/14/2005

BAKER & BOTTS
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/830,530	HO ET AL.	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-43 are pending.

Priority

2. The claim for priority under 35 U.S.C. 119 for PCT/SG99/00105 having a filing date of October 26, 1999 based on Singapore application 9803458-0 filed October 28, 1998 is acknowledged.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on July 17, 2001 has been considered. It is noted that the document nos. and names of the inventors do not match.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-43 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter; the claims are not tangible as none of the steps defined in the claims recite the use of hardware to accomplish the steps. Furthermore, claims 1-29, 32 and 36-42 raise a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment or machine which

would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. The encoding and decoding steps defined in these claims define manipulation steps to generate primary data, secondary data and key values without defining a proper context (the preamble nor the recited steps identify a technological art, environment or machine) for the claimed invention.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 1, 2, 7-15, 20, 25, 27-29, 32, 36, 37 and 39-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch USPN 5,276,738 (hereinafter Hirsch) in view of Menezes et al. Handbook of Applied Cryptography, Chapter 1, "Overview of Cryptography", Chapter 5, "Pseudorandom bits and sequences" and Chapter 7, "Block Ciphers" (hereinafter Menezes).

8. As per claim 1, Hirsch discloses an encoding method (fig. 1A and related text) including steps of:

a. providing primary data including a pseudo-random number sequence (fig. 1A, reference no. 16),

b. providing secondary data including a plurality of second data elements (fig. 1A, reference no. 12) and for each second data elements,

i. performing an operation with a first data element (fig. 1A, reference no. 1), and

ii. generating a key element as a result of the operation wherein each operation is performed and each key element is generated without degrading the primary data (fig. 1A, reference no. 24).

9. Hirsch does not disclose steps of providing primary data, specifically, how the pseudo-random number sequence is derived from the primary data. Menezes discloses generating a pseudo-random number sequence using a DES block cipher (Menezes, pg. 173, section 5.3 "Pseudorandom bit generation", 1st paragraph), which has the following steps:

c. providing an ordered plurality of first data elements, the content of each first data element being represented by a group of digits and reading the groups of digits into an array such that each position in the array contains one of the digits (Menezes, pg. 254, fig. 7.9, "input");

d. selecting a starting position within the array of digits (Menezes, pg. 254, fig. 7.9, "L0" and "R0"; the starting position coincides with the beginning of each register storing the left portion and right potion of the primary data); and

e. regrouping the digits to form new groups of digits with reference to the starting position such that each new group represents a pseudo-random sequence and successive new groups represent the pseudo-random sequence (Menezes, pg. 254, fig. 7.9, "output").

10. It would be obvious to one of ordinary skill in the art at the time the invention was made for the PRNG to utilized the aforementioned steps since the DES algorithm generates a sufficiently secure pseudo-random sequence based on an established block cipher as needed by a secure encoding system. Menezes, pg. 173, section 5.3, 1st paragraph, last sentence. The aforementioned cover the limitations of claim 1.

11. As per claim 2, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Menezes teaches composing functions: a plurality of functions are nested to construct a more complicated function; the simple example of figure 1.8 illustrates taking an ordered set S as input into a first function f which rearranges S to a new ordered set T, which in turn is input to a second function g.

Menezes, pg. 19, section 1.5.3. In the case of a composition of a precursor function with a DES scrambler, the only limitation of such a precursor function is that the number space of its output coincides with the number space of the input for a DES method. (an n-> n mapping) Any permutation function trivially preserves the number space of a DES method as illustrated in the example of fig. 1.8. (DES has a initial permutation step prior to the start of the round operations) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to include a rearranging step prior to generating the pseudo-random number sequence to add more randomness to the cipher and thus devise a more secure function. Menezes, ibid. The aforementioned cover the limitations of claim 2.

12. As per claim 7 and 8, the rejection of claim 2 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the first data elements are rearranged in a predefined manner and in a random or pseudo-random manner. (by virtue of a permutation mapping) The aforementioned cover the limitations of claims 7 and 8.

13. As per claim 9, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Menezes teaches composing functions: a plurality of functions are nested to construct a more complicated function; the simple example of figure 1.8 illustrates taking an ordered set S as input into a first function f which rearranges S to a new ordered set T, which in turn is input to a second function g. Menezes, pg. 19, section 1.5.3. In the case of a composition of a precursor function

with the operations, the only limitation of such a precursor function is that the number space of its output coincides with the number space of the input for the operations. (an n-> n mapping) Any permutation function trivially preserves the number space of the operations as illustrated in the example of fig. 1.8. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to include a rearranging step of the second data elements to add more randomness to the encoded key element and thus devise a more secure method. Menezes, ibid. The aforementioned cover the limitations of claim 9.

14. As per claims 10 and 11, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the technique of resizing one value to match the size of another value is a standard technique in the cryptographic art. For example, the DES cipher implements two steps wherein an expansion permutation expands the contents of the left register from 32 to 48 bits by duplicating bits (pg. 253, 7.82 Algorithm step 3(a)) and a compression permutation truncates the contents of the key value by ignoring every 8^{th} bit (pg. 255, 7.83 Algorithm, step 2); both resizing techniques enable the key values to be combined with the input for processing. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to resize the primary data by truncating the primary data array if the secondary data array is smaller then the primary data array, or repeating the first data elements of the primary data array if the secondary data array is larger than the primary data array, since it enables disjoint values to be processed together using standard resizing techniques as

known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 10 and 11.

15. As per claim 12, the rejection of claims 9 and 11 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, a first rearranging technique on an expanded data set wherein first data elements are repeated, rearranges the first data elements as well as the repeated data elements according to the first technique. The aforementioned cover the limitations of claim 12.

16. As per claim 13, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the first and second data elements are represented by numbers and wherein each operation includes a mathematical operation between the first and second data elements. Hirsch, fig. 1A, ref. no. 14 and related text.

17. As per claim 14, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the first and second data elements are represented in binary notation and each operation includes a logical operation between the first and second data elements. Hirsch, fig. 1A, ref. no. 14 and related text.

18. As per claim 15, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the first and second data elements are represented by

numbers and each operation is a mapping function. Hirsch, fig. 1A, ref. no. 14 and related text.

19. As per claim 20, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the key elements are stored in a key file. Hirsch, fig. 2, ref. no. 400.

20. As per claim 25, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the first data elements are represented in binary notation. Menezes, pg. 253, 7.82 Algorithm, the entries are defined as bits.

21. As per claim 27, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the starting position is selected randomly or pseudo-randomly. Hirsch, col. 5:53-55; claim 5.

22. As per claim 28, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the starting position is selected in a pre-defined manner. Hirsch, col. 2:29-31.

23. As per claim 29, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the primary data includes a random number sequence generated by a random number generator. Hirsch, fig. 1A, reference no. 16.

24. As per claim 32, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the secondary data includes a text message and each second data element includes a character from a character set. Hirsch, col. 2:55-58.

25. As per claims 36 and 37, the rejection of claims 1 and 2 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, a corresponding inverse technique decodes the plurality of key elements to generate the secondary data. Hirsch, col. 7:49-63. The aforementioned cover the limitations of claims 36 and 37.

26. As per claims 39-41, they are claims corresponding to claims 10-12 and 36, and they do not teach or define above the information claimed in claims 10-12 and 36. Therefore, claims 39-41 are rejected as being unpatentable over Hirsch in view of Menezes for the same reasons set forth in the rejections of claims 10-12 and 36.

27. Claims 3, 5, 6, 17, 19, 21, 22, 38 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch in view of Menezes, and further in view of Kajita et al. USPN 5,161,187 (hereinafter Kajita).

28. As per claim 3, the rejection of claim 2 under 35 U.S.C. 103(a) is incorporated herein. (supra) Hirsch is silent on the matter of providing a plurality of techniques for rearranging the first data elements and selecting one technique from the plurality of

techniques. In the analogous art of video scrambling, Kajita discloses a transmitting device wherein signals are scrambled using a plurality of scrambling modes and transmitting the scrambled signal as well as control data that identifies the scrambling mode used to scramble the signal to a receiver, whereupon the receiver uses the control data to identify the correct scrambling mode and descramble the signal. Kajita, col. 2:25-57; 9:25-54. It would be obvious to one of ordinary skill in the art at the time the invention was made for the rearranging technique to be selected from a plurality of techniques, since the selection step increases the level of complexity on the pseudo-random number generation steps to establish a more secure methodology. Kajita, 8:22-51. The aforementioned cover the limitations of claim 3.

29. As per claim 5, the rejection of claim 3 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the selection is made by a user. Kajita, col. 11:13-21.

30. As per claim 6, the rejection of claim 3 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the key elements are stored in a key file. Hirsch, fig. 2, reference nos. 400 and 406. Although Hirsch does not disclose storing information about the selected rearranging technique in an attribute section of the key file, Kajita discloses associating the control data, which contains information about the selected scrambling technique, with the scrambled signal. Kajita, 9:25-34. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to store information about the selected rearranging technique in an attribute section of the key

file, since it enables a receiver of the key file to correctly ascertain the type of technique to decode the key elements as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 6.

31. As per claims 17, 19, 21 and 22, they are claims corresponding to claims 3, 5, 6 and 20, and they do not teach or define above the information claimed in claims 3, 5, 6 and 20. Therefore, claims 17, 19, 21 and 22 are rejected as being unpatentable over Hirsch in view of Menezes and Kajita for the same reasons set forth in the rejections of claims 3, 5, 6 and 20.

32. As per claims 38 and 42, they are claims corresponding to claims 6 and 37, and they do not teach or define above the information claimed in claims 6 and 37. Therefore, claims 38 and 42 are rejected as being unpatentable over Hirsch in view of Menezes and Kajita for the same reasons set forth in the rejections of claims 6 and 37.

33. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch in view of Menezes, and further in view of Ehrsam et al. USPN 3,962,539 (hereinafter Ehrsam).

34. As per claim 26, the rejection of claim 25 under 35 U.S.C. 103(a) is incorporated herein. (supra) The DES operation to produce a pseudo-random number is not defined as a block cipher that permutes primary data values in 8-bit groups; however, other

types of block ciphers are defined this way. For example, Ehrsam discloses a block cipher system that permutes 64-bit message blocks one byte at a time. Ehrsam, col. 6:7-17. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to utilize the block cipher system taught by Ehrsam to produce the pseudo-random sequence, since cryptographic block ciphers are sufficient to remove possible correlations between successive values as required by a secure pseudorandom bit generator. Menezes, pg. 173, section 5.3 "Pseudorandom bit generation",1st paragraph". The aforementioned cover the limitations of claim 26.

35. Claims 4 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch in view of Menezes and Kajita, and further in view of Lee et al. USPN 4,852,023 (hereinafter Lee).

36. As per claim 4, the rejection of claim 3 under 35 U.S.C. 103(a) is incorporated herein. (supra) Neither Hirsch, Menezes nor Kajita suggest that the selection of a technique from a plurality of techniques is to be made randomly or pseudo-randomly. Lee discloses an improvement on a Geffe generator wherein a pseudo-random value is used to key a mux to select between two other pseudo-random sequences to generate a pseudo-random key value. This idea of randomly selecting between a plurality of sources is identified by the inventor to establish a more random key sequence and thus a more secure invention. Lee, col. 2:35-46; 3:12-36. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the selection to be

made randomly or pseudo-randomly, since a randomized control signal generates a greater degree of complexity and randomness and hence a more secure system. Lee, 2:35-37. The aforementioned cover the limitations of claim 4.

37. As per claim 18, it is a claim corresponding to claims 4 and 17, and they do not teach or define above the information claimed in claims 4 and 17. Therefore, claim 18 is rejected as being unpatentable over Hirsch in view of Menezes, Kajita and Lee for the same reasons set forth in the rejections of claims 4 and 17.

38. Claims 23, 24, 30, 31, 33-35 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch in view of Menezes, and further in view of Cooperman et al. USPN 5,613,004 (hereinafter Cooperman).

39. As per claims 23, 24 and 33-35, the rejection of claim 20 under 35 U.S.C. 103(a) is incorporated herein. (supra) Neither Hirsch nor Menezes disclose using a characteristic associated with digital audio samples, still image elements or motion video elements as the primary data to generate a pseudo-random sequence, whereby the primary data and the pseudo-random number is stored in a key file. Cooperman discloses using original content including still digital images, digital audio, and digital video as primary data input to a DES cipher to generate pseudo-random masks, whereby the pseudo-random masks and information matching them to the primary data are stored together for use in decoding. Cooperman, col. 4:32-37; 8:10-18; 9:50-59. It

would be obvious to one of ordinary skill in the art at the time the invention was made for the first data elements to represent a characteristic associated with audio samples, still image elements or motion video elements since these elements are available to the encoding method and are useful input to the generation of a pseudo-random sequence by the DES cipher. Cooperman, 9:50-55. Further, consolidation of pseudo-random number sequence and primary data in a key file are obvious enhancements to ensure that the proper pseudo-random sequence is associated with the corresponding primary data as taught by Cooperman, 8:10-18. The aforementioned cover the limitations of claims 33-35.

40. As per claim 30 and 31, the rejections of claims 23, 24 and 33-35 under 35 U.S.C. 103(a) are incorporated herein. (supra) Although Cooperman does not explicitly disclose the primary data is provided from a file obtained from the Internet, Cooperman discloses using the Internet for the retrieval and transmission of marked digital content including audio and video data. Cooperman, col. 13:65-14:67. Moreover, because the Internet provides secure transmission protocols, such as IPsec, secure transmission of sensitive information such as music and image files are well-established on the Internet at the time the invention was made. Examiner takes Official Notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the primary data to be provided from a file obtained from the Internet to ensure secure delivery of sensitive digital content as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 30 and 31.

41. As per claim 43, it is a claim corresponding to claims 30, 31 and 36, and it does not teach or define above the information claimed in claims 30, 31 and 36. Therefore, claim 43 is rejected as being unpatentable over Hirsch in view of Menezes and Cooperman for the same reasons set forth in the rejections of claims 30, 31 and 36.

Allowable Subject Matter

42. The subject matter of claim 16 is neither taught nor suggested by the prior art of record.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See enclosed PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
June 9, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100